IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF MISSOURI
CENTRAL DIVISION

WILLIAM JOHNSON, et al., individually and on behalf of all others similarly situated,	)	
Plaintiff,	)	
v.	)	Case No. 22-04135-CV-C-BP
CORNERSTONE NATIONAL INSURANCE CO., et al.,	)	
Defendants.	)	

ORDER GRANTING IN PART, DENYING IN PART, AND DEFERRING IN PART DEFENDANTS' MOTIONS TO DISMISS

In this suit, Plaintiffs William Johnson, Joshua Kirk, and Toni Reynolds have asserted claims on behalf of themselves and a putative class (with subclasses) arising from a data breach experienced by Defendant Cornerstone National Insurance Company ("Cornerstone"). Pending are separate Motions to Dismiss filed by Defendants Guidewire Software Inc. ("Guidewire") and Reed-Williams Insurance Agency, Inc. ("Reed-Williams").

Both Moving Defendants argue the claims against them should be dismissed for failure to state a claim. In addition, Reed-Williams argues Plaintiffs lack standing to assert their claims. As discussed below, Guidewire's Motion, (Doc. 59), is **GRANTED IN PART** and **DEFERRED IN PART**, and Reed-Williams's Motion, (Doc. 73), is **GRANTED IN PART**, **DENIED IN PART**, and **DEFERRED IN PART**.[1]

[1] The Docket Sheet does not clearly reflect prior events in this case. On September 28, 2023, Plaintiffs sought leave to file (1) an Amended Complaint under seal and (2) a redacted version for public viewing. (Doc. 40.) This request was granted the next day by the Honorable Willie J. Epps, Jr., to whom the case was assigned at the time. (Doc. 41.) Plaintiffs filed the redacted version of their Amended Complaint on October 12, 2023, (Doc. 42), but did not contemporaneously file the unredacted version under seal. On February 26, 2024, another Defendant, James Insurance Agency, Inc., was dismissed at Plaintiffs' request. (Doc. 90; Doc. 99.) Plaintiffs filed the unredacted Amended Complaint under seal on April 8, 2024. (Doc. 114.) Nonetheless, the Amended Complaint has been the operative pleading since the redacted version was filed in October 2023, and James Insurance Agency remains dismissed.

I. BACKGROUND

Cornerstone provides automobile and homeowners insurance in multiple states around the country, and its policies are sold by independent agents. (Doc. 114, ¶¶ 5, 27.) Accordingly, the independent agents can connect to, and access, Cornerstone's computer system. (Doc. 114, ¶ 5.) "Guidewire provides the subscription services connecting the agents with Cornerstone's databases," (Doc. 114, ¶ 5), and it and Cornerstone together (and solely) designed the system accessed by agents. (Doc. 114, ¶¶ 6, 97.) Information accessible by agents includes personal information from drivers' license records, (Doc. 114, ¶¶ 6, 28), which is understandable given that Cornerstone sells automobile insurance.[2]

In November 2021, Cornerstone learned one or more unauthorized third parties had gained access to its system through some of its agents' accounts. (Doc. 114, ¶ 34.) It issued a "global password reset" and investigated the matter, ultimately confirming individuals' names and driver's license numbers may have been accessed by unauthorized persons. (Doc. 114, ¶ 34.) Reed-Williams was one of the points of entry; that is, its user account was among those utilized by the unauthorized user(s) to gain access to Cornerstone's system. (Doc. 114, ¶ 8.) Information for nearly 300,000 people was exposed as a result of this breach. (Doc. 114, ¶ 38.)

Generally, the Amended Complaint alleges Defendants created the conditions enabling the unauthorized access to Plaintiffs' data, and in doing so they breached various common law and

Separate Defendant Accredited Resource Insurance Agency was dismissed without prejudice after the filing of the sealed version of the Amended Complaint. (Doc. 118.)

[2] It is not clear from the Amended Complaint whether (1) Cornerstone's computer system stored driver's license information or (2) access to Cornerstone's computer system in turn provided access to state computer systems containing driver's license information.

statutory duties. The specific claims are listed below; they are asserted by all three Plaintiffs against all three remaining Defendants unless otherwise indicated:[3]

Count I	Violation of the federal Drivers' Privacy Protection Act, (the "DPPA");
Count II	Negligence;
Count III	Negligence per se;
Count IV	Violation of the California Consumer Privacy Act (asserted by Johnson and Reynolds only, against Cornerstone and Guidewire only)
Count V	Violation of the California Unfair Competition Law (asserted by Johnson and Reynolds only); and
Count VIII	Breach of contract (asserted against Guidewire only and based on Plaintiffs' alleged status as third-party beneficiaries of the contract between Guidewire and Cornerstone).

Additional allegations from the Amended Complaint will be discussed as necessary to resolve the issues raised by the parties.

II. DISCUSSION

A. Standing

Article III of the Constitution requires that plaintiffs have standing to assert their claims, *e.g.*, *Lujan v. Defenders of Wildlife*, 504 U.S. 555, 560 (1992), and the Court "has an independent obligation to assure that standing exists, regardless of whether it is challenged by any of the parties." *Summers v. Earth Island Inst.*, 555 U.S. 488, 499 (2009). Therefore, while the issue is raised only by Reed-Williams, the Court's discussion on this issue applies to all Defendants.

[3] There is no Count VI. Count VII seeks declaratory and injunctive relief, but, contrary to Plaintiffs' argument, the Declaratory Judgment Act, 28 U.S.C. § 2201, is not an independent cause of action. *E.g.*, *Wilton v. Seven Falls Co.*, 515 U.S. 277, 288 (1995) ("By the Declaratory Judgment Act, Congress sought to place a remedial arrow in the district court's quiver; it created an opportunity, rather than a duty, to grant a new form of relief to qualifying litigants."); *Skelly Oil Co. v. Phillips Petroleum Co.*, 339 U.S. 667, 671 (1950) ("The operation of the Declaratory Judgment Act is procedural only." (cleaned up)); *First Fed. Sav. & Loan Ass'n of Harrison, Ark. v. Anderson*, 681 F.2d 528, 533 (8th Cir. 1982) ("It is well settled that the declaratory judgment statute is strictly remedial in nature and does not provide a separate basis for subject matter jurisdiction."). Accordingly, neither Count VI nor Count VII needs to be discussed further.

"[T]he irreducible constitutional minimum of standing consists of three elements. The plaintiff must have (1) suffered an injury in fact, (2) that is fairly traceable to the challenged conduct of the defendant, and (3) that is likely to be redressed by a favorable judicial decision." *Spokeo, Inc. v. Robins*, 578 U.S. 330, 338 (2016) (quotation omitted). The Court addresses each requirement in turn.

1. Injury In Fact

An injury in fact must be actual or imminent and must also be concrete and particularized. *E.g.*, *id*. at 339. "An allegation of future injury may suffice if the threatened injury is 'certainly impending,' or there is a 'substantial risk' that the harm will occur." *Susan B. Anthony List v. Driehaus*, 573 U.S. 149, 158 (2014) (cleaned up). As particularly relevant here, standing may be "based on a 'substantial risk' that . . . harm will occur, which may prompt plaintiffs to reasonably incur costs to mitigate or avoid that harm." *Clapper v. Amnesty Int'l USA*, 568 U.S. 398, 409 n.5 (2013); *see also TransUnion LLC v. Ramirez*, 594 U.S. 413, 436 (2021); *In re SuperValu, Inc.*, 870 F.3d 763, 769 (8th Cir. 2017) ("*SuperValu*").

Here, Plaintiffs allege the data breach exposes them to a substantial risk of identity theft. Whether the risk of identity theft constitutes an injury depends on the "substance of the allegations" in the Amended Complaint. *SuperValu*, 870 F.3d at 769. The Second Circuit and the Third Circuit recently surveyed judicial decisions (including *SuperValu*) and identified certain common considerations for determining if the alleged risk of identity theft is sufficient to constitute an injury for standing purposes. "First, and most importantly, our sister circuits have consistently considered whether the data at issue has been compromised as the result of a targeted attack intended to obtain the plaintiffs' data." *McMorris v. Carlos Lopez & Assocs., LLC*, 995 F.3d 295, 301 (2d Cir. 2021); *see also Clemens v. ExecuPharm Inc.*, 48 F.4th 146, 153 (3d Cir. 2022). This

factor is relevant because a targeted attack suggests the hacker/thief intends to use the stolen data for malicious purposes. "Second, . . . courts have been more likely to conclude that plaintiffs have established a substantial risk of future injury where they can show that at least some part of the compromised dataset has been misused . . . ." *McMorris*, 995 F.3d at 301; *see also Clemens*, 48 F.4th at 153-54. If some of the information has been misused, courts are more likely to conclude there is a substantial risk that misuse will continue. "Finally, courts have looked to the type of data at issue, and whether that type of data is more or less likely to subject plaintiffs to a perpetual risk of identity theft or fraud once it has been exposed." *McMorris*, 995 F.3d at 302; *see also Clemens*, 48 F.4th at 154.

Here, the Complaint alleges there was a targeted effort directed at Cornerstone's computers, and information for nearly 300,000 people was taken. (*E.g.*, Doc. 114, ¶¶ 8, 38.) The information at issue—driver's license data and associated names—is allegedly sought by hackers because it can be used to forge identifying information or otherwise engage in identity theft. (*E.g.*, Doc. 114, ¶¶ 44-46, 51-57, 60, 62-64.) "Stolen driver's licenses can be used (alone or in combination with other information) by malicious actors to," among other things, obtain credit cards or loans, open bank accounts, rent cars, apply for government benefits, and redirect mail. (Doc. 114, ¶ 46.) Finally, one of the Plaintiffs (Kirk) experienced two incidents suggesting his information had been misused. In January 2022—in the midst of the period during which Cornerstone's database was hacked—Kirk learned an unauthorized person applied for a loan in his name. (Doc. 114, ¶ 122.) And, in July 2022—approximately three weeks after the hack ended—Kirk was contacted about a car he had supposedly rented but not returned. (Doc. 114, ¶ 123.)

Thus, (1) the circumstances indicating the information was taken with malicious intent, (2) the nature of the information taken, and (3) the fact some of the information appears to have been used maliciously combine to demonstrate a substantial risk Plaintiffs will suffer identity theft. Moreover, where there is a substantial risk of harm, the time and energy spent by Plaintiffs guarding against that risk, (*see* Doc. 114, ¶¶ 105, 111), constitutes an injury as well. *E.g.*, *Clemens*, 48 F.4th at 155-56; *In re Equifax Inc. Customer Data Sec. Breach Litig.*, 999 F.3d 1247, 1263 (11th Cir. 2021).

Reed-Williams characterizes this analysis as inconsistent with *SuperValu*, describing the case as requiring actual misuse of Plaintiffs' data. (Doc. 74, p. 11.) Setting aside the fact that Kirk has alleged actual misuse of his data, the Court disagrees with this interpretation of *SuperValu*. In that case, the stolen data consisted of credit card numbers. The plaintiffs alleged injury from (1) the risk of identity theft and (2) actual fraudulent charges. In its discussion about the risk of identity theft (under the heading "Future Injury"), the Eighth Circuit did not hold that establishing a substantial risk of *future* identity theft required an allegation of *past* actual misuse. *See SuperValu*, 870 F.3d at 768-72. Instead, it noted the plaintiffs relied on a Government Accountability Office ("GAO") report to establish that risk, but the report established credit card information could not be used to open new accounts and (at most) could be used to make unauthorized charges. *Id*. at 770-71. Thus, *SuperValu* highlights the importance of the third factor identified by the Second and Third Circuits: credit card numbers—which can be canceled to reduce (or eliminate) the risk of unauthorized charges—pose less (or an insubstantial) risk of future harm as compared to other forms of personal information. *SuperValu* did not hold that actual misuse of personal information is required for there to be a substantial risk of future harm.

Reed-Williams also points to two decisions from the Northern District of California in *Greenstein v. Noblr Reciprocal Exchange* ("*Greenstein*"). In that case, an insurance company's computers were hacked, and customers' driver's license data was stolen. In February 2022, the District Court dismissed the First Amended Complaint (with leave to amend) because it did not establish standing for the plaintiffs, explaining that "driver's license numbers do not provide hackers with a clear ability to commit fraud and are considered not as sensitive as social security numbers." *Greenstein*, 585 F. Supp. 3d 1220, 1227 (N.D. Cal. 2022). In December 2022, the District Court dismissed the Second Amended Complaint; it acknowledged the plaintiffs had presented "new arguments as to why driver's license data should be considered sensitive [personal information] for standing purposes" but "continue[d] to hold that driver's license numbers are not as sensitive as social security numbers, and that they do not rise to the level of sensitive [personal information] needed to establish a credible and imminent threat of future harm." *Greenstein*, 2022 WL 17418972, at *2 (N.D. Cal. Dec. 5, 2022). However, not only is this decision on appeal, but the Court does not know what facts were alleged in either the First Amended Complaint or the Second Amended Complaint. There is no value in comparing various complaints from different cases to determine how similar or dissimilar they are to the case at bar. Mindful that each case turns on the allegations before the Court (and not the allegations before other courts), *see SuperValu*, 870 F.3d at 769, the Court believes it proper to focus on the Amended Complaint's allegations.[4] And as explained, the paragraphs cited previously, (Doc. 114, ¶¶ 44-46, 51-57, 60, 62-64), sufficiently allege a risk of identity theft.

[4] The Court further observes that Kirk's allegations of an unauthorized car rental and an unauthorized loan application, while unique to him, may be injuries sufficient to support standing. However, those injuries would not support standing for Johnson or Reynolds, so in the interest of clarity the Court will not discuss the possibility further.

For these reasons, the Court concludes the facts in the Amended Complaint establish a substantial risk that Plaintiffs will be subjected to future harm. The Amended Complaint also alleges that, because of that risk, Plaintiffs have incurred and will incur expenses to guard against that identity theft. Accordingly, Plaintiffs have demonstrated they have suffered an injury as required to establish standing.

2. Traceability

The traceability requirement is satisfied if there is alleged to be a causal connection between the injury and the defendant's conduct. *See*, *e.g.*, *Bennett v. Spear*, 520 U.S. 154, 162 (1997); *Lujan*, 504 U.S. at 560. A factual connection, not a legal connection, is required. *E.g.*, *Department of Commerce v. New York*, 139 S. Ct. 2551, 2566 (2019); *Bennett*, 520 U.S. at 168-69. The plaintiff's burden is "relatively modest" at the pleading stage. *SuperValu*, 870 F.3d at 772 (quoting *Bennett*, 520 U.S. at 171).

Reed-Williams argues there is no connection between the data breach and the unauthorized transactions in Kirk's name, in that nothing establishes those applications were made possible by information improperly taken from Cornerstone's system. But as discussed before, the unauthorized transactions only serve a role in determining whether there is a substantial risk of future harm. In that context, the unauthorized transactions are not the injury; the risk of future identity theft is the injury, and there is no argument that the increased risk is not traceable to Defendants. Contrary to Reed-Williams' argument, there is no need for Plaintiffs to allege—at this stage of the proceedings—specific proof establishing a connection between the unauthorized transactions and Defendants' conduct. *See SuperValu*, 870 F.3d at 772.

The Court thus concludes Plaintiffs have adequately alleged their injuries are traceable to Defendants' conduct.

3. Redressability

In contending Plaintiffs have not established that their injuries are redressable, Reed-Williams primarily reiterates its arguments contending Plaintiffs have not alleged an injury, (Doc. 74, p. 13), so further discussion is not required. Reed-Williams also suggests injunctive relief will not provide redress because an injunction could not compel the hackers to return the information. (Doc. 74, pp. 13-14.) However, as explained earlier, Plaintiffs' injuries include their costs associated with preventing the identity theft, and that injury can be redressed.

4. Conclusion[5]

The Court concludes Plaintiffs have alleged a substantial risk of identity theft, which qualifies as an injury for purposes of Article III standing. It also concludes Plaintiffs have alleged the injuries are fairly traceable to Defendants' conduct and are redressable. Accordingly, Plaintiffs have standing to assert their claims, and the case will not be dismissed for lack of jurisdiction.

B. Failure to State a Claim

Under Rule 12(b)(6), the Court "must accept as true all of the complaint's factual allegations and view them in the light most favorable to the Plaintiff[ ]." *Stodghill v. Wellston School Dist.*, 512 F.3d 472, 476 (8th Cir. 2008); *see also Alexander v. Hedback*, 718 F.3d 762, 765 (8th Cir. 2013).

> To survive a motion to dismiss, a complaint must contain sufficient factual matter, accepted as true, to state a claim to relief that is plausible on its face. A claim has facial plausibility when the plaintiff pleads factual content that allows the court to draw the reasonable inference that the defendant is liable for the misconduct alleged. The plausibility standard is not akin to a probability requirement, but it asks for more than a sheer possibility that a defendant has acted unlawfully. Where

[5] At times, Plaintiffs seem to (1) allege Defendants continue to utilize ineffective protective measures and (2) seek injunctive relief requiring Defendants to utilize better protective measures. However, they do not clearly present this position, so the Court does not consider its potential utility in this case. The Court also finds it unnecessary to address *Heglund v. Aitkin County*, 871 F.3d 572 (8th Cir. 2017), which (1) discusses standing for claims under the DPPA specifically and (2) was not mentioned by the parties.

> a complaint pleads facts that are merely consistent with a defendant's liability, it stops short of the line between possibility and plausibility of entitlement to relief.

Ashcroft v. Iqbal, 556 U.S. 662, 678 (2009) (quotations and citations omitted); *see also Bell Atlantic Corp. v. Twombly,* 550 U.S. 544, 570 (2007); *Horras v. American Capital Strategies, Ltd.*, 729 F.3d 798, 801 (8th Cir. 2013). In making this evaluation, the Court is limited to a review of the Complaint, exhibits attached to the Complaint, and materials necessarily embraced by the Complaint. *E.g., Mattes v. ABC Plastics, Inc.,* 323 F.3d 695, 697 n.4 (8th Cir. 2003).

However, "the tenet that a court must accept as true all of the allegations contained in a complaint is inapplicable to legal conclusions. Threadbare recitals of the elements of a cause of action, supported by mere conclusory statements, do not suffice." *Iqbal,* 556 U.S. at 678. This point is particularly important because the Amended Complaint presents many legal conclusions; the Court has not accorded them any consideration in determining if a claim has been stated.

For ease of discussion, the Court will discuss (1) the DPPA claim, then (2) the two California statutory claims separately, and then (3) the three common law claims together.

1. Count I – The DPPA

The DPPA provides that "[a] person who knowingly . . . discloses . . . personal information, from a motor vehicle record, for a purpose not permitted under [the DPPA] shall be liable to the individual to whom the information pertains . . . ." 18 U.S.C. § 2724(a). There is no dispute that the Amended Complaint alleges information from a motor vehicle record was disclosed; the question is whether the Amended Complaint alleges Defendants disclosed the information "knowingly." The Court concludes it does not.

Defendant argues that under the DPPA, a party acts knowingly if it voluntarily discloses information; while the Eighth Circuit has not addressed the issue, for purposes of discussion the Court accepts this as correct. *See Senne v. Village of Palatine*, 695 F.3d 597, 603 (7th Cir. 2012).

Plaintiffs argue this requirement is satisfied by its allegations that the driver's license information was voluntarily transmitted to those who accessed Cornerstone's system, regardless of how they accessed it. The Court is not persuaded by this argument because it ignores the entirety and context of the facts alleged.

Viewed in the light most favorable to Plaintiffs, the Amended Complaint alleges Cornerstone voluntarily disclosed information to those with access to its system. Critically, however, the Amended Complaint alleges Defendants controlled (or at least attempted to control) who had access to the system. (*E.g.*, Doc. 114, ¶¶ 8, 34, 223 (discussing passwords used to access Cornerstone's system); Doc. 114, ¶¶ 5, 25, 34, 73, 259 (describing how agents had a "subscription" to Cornerstone's system).) Defendants did not voluntarily give hackers access to Cornerstone's system, nor did they voluntarily make Plaintiffs' information (or access to the system) available to the public.[6] And because the Amended Complaint cannot be construed as alleging Defendants knowingly gave protected information to the hackers, it does not state a claim under the DPPA.[7]

2. Count IV – California Consumer Privacy Act

The California Consumer Privacy Act (the "CCPA") imposes duties on certain businesses to protect individuals' personal information. It also provides a private right of action for any person whose personal information "is subject to an unauthorized access and exfiltration, theft, or

[6] This point distinguishes the cases Plaintiffs rely on. In those cases, the defendants allegedly permitted anyone to access information from their systems. *See In re GEICO Customer Data Breach Litig.*, 2023 WL 5524105, at *3-4 (E.D.N.Y. Aug. 28, 2023) (Insurance company's website's "auto-populate feature" provided information to members of the public); *Stallone v. Farmers Grp., Inc.*, 2022 WL 10091489, at *10 (D. Nev. Oct. 15, 2022) (Information could be obtained simply by entering a person's name, address, and date of birth); *In re USAA Data Sec. Litig.*, 621 F. Supp. 3d 454, 468 (S.D.N.Y. 2022) ("USAA's voluntary decision to automatically pre-fill its quote forms with driver's license numbers constitutes a 'knowing disclosure' of personal information."). Moreover, it seems inconsistent with the ordinary meaning of the words to hold that a party "voluntarily disclosed" protected information when, in fact, it was stolen. *See, e.g.*, *Enslin v. The Coca-Cola Co.*, 136 F. Supp. 3d 654, 671 (E.D. Pa. 2015)

[7] An analogy may help prove the point. If Defendants placed confidential information in a safe, it could be said that they provided access to anyone to whom they voluntarily gave the key. However, if the key was stolen—thereby giving the thief access—one would not characterize Defendants as having voluntarily provided the thief access to the safe's contents.

disclosure as a result of the business's violation of the duty to implement and maintain reasonable security procedures and practices . . . to protect the personal information . . . ." Cal. Civil Code § 1798.150(a)(1). A "business", as defined by the CCPA, may be liable in such a suit; the issue is whether Guidewire satisfies the CCPA's definition of a "business."

A company qualifies as a "business" under the CCPA if, *inter alia*, it "collects consumers' personal information, or on the behalf of which such information is collected and that alone, or jointly with others, determines the purposes and means of the processing of consumers' personal information." Cal. Civ. Code § 1798.140(d)(1). Parsing the definition reveals that, for the Amended Complaint to state a claim against Guidewire, it must allege facts demonstrating:

1. Guidewire collected personal information, or that personal information was collected on its behalf, *and*
2. Alone or with others, Guidewire determined the purposes and means of processing the personal information.

Guidewire contends neither requirement is established in the Amended Complaint; the Court focuses on the first requirement.

The CCPA defines "collect" to mean "buying, renting, gathering, obtaining, receiving, or accessing any personal information pertaining to a consumer by any means." Cal. Civ. Code 1798.140(f). In opposing dismissal, Plaintiffs argue Guidewire "collected" information because it "accessed" it, but the Amended Complaint does not support this theory.[8] Plaintiffs cite paragraphs from the Amended Complaint alleging Guidewire set up Cornerstone's system and its controls, (Doc. 114, ¶¶ 7, 8, 25, 28, 36, 72, 173, 192, 213); however, in concert, these paragraphs

[8] Plaintiffs do not suggest Guidewire "collected" personal information by buying, renting, gathering, obtaining, or receiving it, and the Amended Complaint would not support such an argument in any event. Therefore, the Court does not discuss these aspects of the definition.

do not allege Guidewire itself actually "accessed" Plaintiffs' (or anyone's) confidential information. Other paragraphs not cited by Plaintiffs confirm the point: (1) Guidewire helped design and set up Cornerstone's system, (2) part of the design allowed Cornerstone to determine who could access its system, and (3) access to Cornerstone's system provides access to individuals' confidential information. (*E.g.*, Doc. 114, ¶¶ 5-6, 74, 97-98, 183.) But these actions—including designing a system for Cornerstone that allowed it or others to access information—do not themselves constitute "accessing" information, and the Amended Complaint does not allege Guidewire accessed confidential information. Plaintiffs correctly point out that a company providing services to a business can also be a "business" under the CCPA, (Doc. 103, pp. 22-23); however, the Amended Complaint does not allege any facts that would allow Guidewire to qualify as such.

The Amended Complaint does not allege facts plausibly demonstrating Guidewire "collected" personal information within the meaning of the CCPA, and thus fails to allege Guidewire is a "business" within the meaning of the CCPA. Therefore, Plaintiffs' CCPA claim against Guidewire must be dismissed.[9]

3. Count V – California Unfair Competition Law

California's Unfair Competition Law ("UCL") permits suit against those who engage in "unfair competition," which "mean[s] and include[s] any unlawful, unfair or fraudulent business act or practice . . . ." Cal. Bus. & Prof. Code § 17200. Suit may be brought by, *inter alia*, "a person who has suffered injury in fact and has lost money or property as a result of the unfair competition." *Id*. § 17204. Finally, "the remedy for a UCL violation is either injunctive relief or

[9] The Court's discussion makes it unnecessary to consider Guidewire's other arguments in favor of dismissing Count IV.

restitution." *Fresno Motors, LLC v. Mercedes Benz USA, LLC*, 771 F.3d 1119, 1135 (9th Cir. 2014) (citing Cal. Bus. & Prof. Code § 17203). The Moving Defendants contend the UCL claim must be dismissed because the Amended Complaint does not adequately allege (1) they engaged in unlawful, unfair, or fraudulent conduct or (2) Plaintiffs suffered losses for which the UCL provides a remedy. However, before considering these arguments, the Court directs the parties to fully address an issue that cannot be addressed based on the current briefing.

In its Reply Suggestions, Reed-Williams argues the UCL does not apply to conduct occurring outside California. The Court does not ordinarily consider issues raised for the first time in a party's Reply Suggestions, but this appears to be a significant and straightforward issue that will need to be addressed eventually, so further briefing is warranted.

California courts presume statutes do not apply "with respect to occurrences outside the state, unless such intention is clearly expressed or reasonably to be inferred from the language of the act or from its purpose, subject matter or history." *Sullivan v. Oracle Corp.*, 254 P.3d 237, 248 (Cal. 2011) (cleaned up). "Neither the language of the UCL nor its legislative history provides any basis for concluding the Legislature intended the UCL to operate extraterritorially. Accordingly, the presumption against extraterritoriality applies to the UCL in full force." *Id*.

In *Sullivan*, the California Supreme Court considered a UCL claim based on the failure to pay wages required by the Fair Labor Standards Act ("FLSA").[10] It held the UCL did not apply to a claim brought by workers outside California against a California corporation simply because the decision to pay wages was made in California. *Id*. at 247-48. In contrast, the UCL could apply if the policy was effectuated (i.e., the employees were paid) in California, because that is where the challenged *conduct* occurred. *Id*. at 249. Given that the critical question is whether the

[10] The issue arose because the plaintiffs sought to take advantage of the UCL's statute of limitations, which is longer than the FLSA's.

wrongful conduct occurred in California, it does not appear the UCL applies when (1) a policy was adopted in California (2) to govern conduct outside California. *Id*. at 248 n.10; *see also, e.g., Oman v. Delta Airlines, Inc.*, 889 F.3d 1075, 1079 (9th Cir. 2018) ("If the conduct that 'creates liability' occurs in California, California law properly governs that conduct. By contrast, if the liability-creating conduct occurs outside of California, California law generally should not govern that conduct . . . ." (cleaned up)); *People v. Ashford Univ., LLC*, 100 Cal. App. 5th 485, 319 Cal. Rptr. 3d 132, 167 (2024) (Differentiating *Sullivan* because there was "evidence defendants committed the misconduct . . . inside California"); *Norwest Mortg., Inc. v. Superior Ct.*, 72 Cal. App. 4th 214, 222, 85 Cal. Rptr. 2d 18, 23 (1999) ("[W]e do not construe a statute as regulating occurrences outside the state unless a contrary intention is clearly expressed or reasonably can be inferred from the language or purpose of the statute.").

This issue is particularly relevant with respect to Reed-Williams, given that (1) it is an Oklahoma corporation with its principal office in that state, (Doc. 114, ¶ 18), (2) Cornerstone's servers are allegedly in Missouri, (Doc. 114, ¶ 259), and (3) Reed-Williams is not alleged to have entered a business relationship with Plaintiffs (or, for that matter, anyone in California), or engaged in any conduct in California. Moreover, even though Guidewire is a California corporation, the UCL may not apply because its wrongful conduct—creating a system for Cornerstone in Missouri—did not occur in California.

As stated, Reed-Williams first raised this issue in its Reply Suggestions, and then only briefly. (Doc. 111, pp. 11-12.) Guidewire did not discuss the issue at all; however, given that the Court intends to permit Reed-Williams to discuss the issue further, it makes sense to permit Guidewire to do the same. Accordingly, on or before May 15, 2024, if Guidewire and Reed-Williams wish the Court to consider the issue, they must file a Supplemental Brief that fully

addresses it. Plaintiffs shall have fourteen days to respond, and Guidewire and Reed-Williams will have fourteen days thereafter to reply. In its opposition, Plaintiffs must specifically identify the Amended Complaint's allegations describing Guidewire's and Reed-Williams's conduct in California.

4. The Common Law Claims

As stated earlier, Plaintiffs' claims include three common law claims (negligence, negligence per se, and breach of contract, the latter of which is asserted only against Guidewire). In arguing for dismissal of the common law claims, Guidewire relied on California law, while Reed-Williams relied on Missouri law. In their response, Plaintiffs suggested Missouri law applies, (*e.g.*, Doc. 103, p. 20), yet generally did not rely on Missouri law and instead cited law from other jurisdictions. (*See, e.g.*, Doc. 103, pp. 12-13 & n.3, 18-19; Doc. 105, pp. 16-17 & n.6, 20-21.) In its Reply Suggestions, Guidewire observes "Plaintiffs offer no reason why Missouri law should govern the claims that they—residents of Tennessee and California—assert against Guidewire, a California-headquartered corporation." (Doc. 113, p. 10.) The Court shares this observation; in fact, it goes further and notes Reed-Williams is an Oklahoma corporation with its principal place of business in that state, (Doc. 114, ¶ 18), meaning there is a possibility Oklahoma law governs the common law claims asserted against it.

"Federal courts sitting in diversity apply the choice-of-law rules of the forum state." *Eagle Tech. v. Expander Americas, Inc.*, 783 F.3d 1131, 1137 (8th Cir. 2015). There is no need to conduct a choice of law analysis if the choice would not affect the outcome. *E.g.*, *Prudential Ins. Co. of Am. v. Kamrath*, 475 F.3d 920, 924 (8th Cir. 2007). Here, the Court has not been presented with any reason to believe Missouri, Tennessee, Oklahoma, and California common law are the same on all the relevant issues; to the contrary, there is reason to think they are not. For instance,

Guidewire argues negligence per se is not an independent cause of action under California law. (Doc. 68, p. 18.) Plaintiffs concede Guidewire has correctly stated California law on this point but counter by arguing the law in Missouri is different. (*See* Doc. 103, p. 20.) Another example appears in the parties' arguments about Count VIII: Guidewire relies on California law to argue Plaintiffs have not stated a claim for breach of contract, (*see* Doc. 68, pp. 25-56), and Plaintiffs fault Guidewire's reliance on California law while citing decisions applying Minnesota, Pennsylvania, and Indiana law. (Doc. 103, pp. 27-29.) Moreover, before the Court considers complicated issues such as (1) the economic loss doctrine and (2) the extent to which a defendant can be liable for the wrongful/criminal acts of others, it wishes to ensure it is applying the law from the correct jurisdiction.

Accordingly, on or before May 15, 2024, Guidewire and Reed-Williams must file a Supplemental Brief that (1) conducts a choice of law analysis and (2) restates their arguments for dismissal of Counts II, III, and VIII, applying the appropriate state's law. Plaintiffs shall have fourteen days to respond, and Guidewire and Reed-Williams will have fourteen days thereafter to reply. The parties' filings on these issues should be combined with any arguments they make regarding the UCL claim, as discussed above.

III. CONCLUSION

For the reasons stated above, Guidewire's Motion is **GRANTED IN PART** and **DEFERRED IN PART**, and Reed-Williams's Motion is **GRANTED IN PART**, **DENIED IN PART**, and **DEFERRED IN PART**. Specifically,

1. Reed-Williams's Motion is **DENIED** to the extent it asks that the case be dismissed for lack of jurisdiction, **GRANTED** to the extent it seeks dismissal of Count I, and **DEFERRED** to the extent it seeks dismissal of Counts II, III, and V;

2. Guidewire's Motion is **GRANTED** to the extent it seeks dismissal of Counts I and IV, and **DEFERRED** to the extent it seeks dismissal of Counts II, III, V, and VIII; and

3. The parties shall submit supplemental briefing with respect to Counts II, III, V, and VIII as set forth in Parts II(B)(3) and II(B)(4), above.

IT IS SO ORDERED.

/s/ Beth Phillips
BETH PHILLIPS, CHIEF JUDGE
UNITED STATES DISTRICT COURT

DATE: April 29, 2024